

**Listing of the Claims:**

The following is a complete listing of all the claims in the application, with an indication of the status of each:

- 1        1 (Currently Amended). A method for selectively denying access to encoded data, said method comprising the steps of:
  - 3                loading an encryption key into a mission planning workstation at a first location;
  - 5                connecting ~~at least one~~ a media device to a said mission planning workstation located at a "home base", wherein ~~each media device is~~ capable of connections with both the mission planning workstation and a target portable computing device, the portability being enabled by transport of the computing device by a land, air, sea or space vehicle during a mission;
  - 11                loading said encryption key from said mission planning workstation into said media device;
  - 13                encrypting sensitive data using ~~an~~ said encryption key;
  - 14                loading the encrypted data onto ~~at least one~~ one of the media devices device;
  - 16                loading unencrypted data onto ~~at least one~~ one of the ~~a~~ media devices device, wherein data necessary to enable ~~the vehicle and~~ a target portable computing device associated with a vehicle to return to a location selected as a mission end location remains unencrypted;
  - 20                disconnecting ~~each of the~~ at least one said media devices device from the mission planning workstation;
  - 22                connecting ~~each of the~~ at least one a media devices device to the target portable computing device;
  - 24                powering up the target portable computing device, thereby enabling it to execute a desired program or process;
  - 26                transferring said encryption key to volatile memory from said

27       media device;  
28              transporting the target portable computing device and media  
29        devices ~~via a land, air, space or sea vehicle~~ to a location physically distant  
30       from the mission planning workstation, thereby ~~commencing the mission;~~  
31              deleting said encryption key from said media device in response to  
32       said transport step;  
33              maintaining said encryption key only in volatile memory after said  
34       deleting step; and  
35              providing the vehicle operator or pilot, or other mission personnel  
36       traveling with the vehicle, a means to delete ~~deleting~~ the encryption key  
37       from volatile memory resident on the target portable computing device in  
38       the event of a threat, whether perceived or real ~~responsive to an operator;~~  
39       and or  
40              providing a means to automatically ~~delete~~ deleting the encryption  
41       key from volatile memory resident on the target portable computing device  
42       in the event of a loss of power to the target portable computing device.

2 (Canceled).

1       3 (Currently Amended). A method as recited in claim 2-1, wherein the  
2       step of deleting the encryption key responsive to an operator overwrites the  
3       location in non-volatile memory where the encryption key previously  
4       resided a desired number of times.

1       4 (Currently Amended). A method as recited in claim 2-1, wherein the  
2       step of deleting is triggered by an indication that ~~the~~ a vehicle used for  
3       transporting the target portable computing device has left ~~the~~ a home base.

1       5 (Currently Amended). A method as recited in claim 1, wherein the step  
2       of encrypting sensitive data further comprises the steps of:

3           selecting an encryption key, wherein the encryption key comprises  
4        a number of bits sufficient to prohibit an unauthorized person from  
5        "breaking" the encryption key at a desired level of difficulty; and  
6           ~~loading the selected encryption key into non-volatile memory on~~  
7        ~~one of the at least one media devices.~~

1        6 (Original). A method as recited in claim 5, wherein an operator of the  
2        target portable computing device has no knowledge of the encryption key  
3        used to encrypt data on the at least one media device in the encrypting step,  
4        and the encryption key is maintained at the home base mission planning  
5        workstation.

1        7 (Original). A method as recited in claim 5, wherein the step of selecting  
2        an encryption key selects a new key on a desired periodic basis, thereby  
3        minimizing a risk of compromise of a previously used encryption key.

1        8 (Currently Amended). A method as recited in claim 1, further  
2       comprising the steps of: wherein said deleting step responsive to an  
3       operator is performed upon  
4           perceiving a threat by a member of the mission; ~~and~~  
5           ~~deleting the encryption key using means providing the vehicle~~  
6           ~~operator or pilot, or other mission personnel traveling with the vehicle, a~~  
7           ~~means to delete the encryption key.~~

1        9 (Original). A method as recited in claim 8, further comprising the step of  
2        transporting the vehicle to the selected mission end location, wherein  
3        encrypted data remains encrypted and unencrypted data enables the vehicle  
4        to operate at with sufficient performance to arrive at the mission end  
5        location.

10 (Canceled).

1       11 (Original). A method as recited in claim 10, further comprising the step  
2       of transporting the vehicle to the selected mission end location, wherein  
3       encrypted data remains encrypted and unencrypted data enables the vehicle  
4       to operate at with sufficient performance to arrive at the mission end  
5       location.

1       12 (Currently Amended). A system for selectively denying access to  
2       encoded data, comprising:

3               a selected encryption key, the key being of a number of bits  
4       sufficient to deter compromise of sensitive data to a desired difficulty  
5       level;

6               a target portable computing device loaded onto a land, sea, air or  
7       space vehicle, the target portable computing device used for mission  
8       specific tasks and having connections for at least one media device,  
9       wherein sensitive encrypted data and/or unencrypted benign data is to be  
10      loaded on the at least one media device depending on mission parameters,  
11      the target computing device comprising:

12               means to delete the encryption key from volatile memory  
13       resident on the target portable computing device in the event of a  
14       threat, whether perceived or real responsive to an operator; and

15               means to automatically delete the encryption key from  
16       volatile memory resident on the target portable computing device  
17       in the event of a loss of power to the target portable computing  
18       device;

19               a mission planning computer workstation connected to at least one  
20       media device during loading and encryption of sensitive data, and loading  
21       of unencrypted benign data, wherein the encryption key is loaded into the at  
22       least one media device and erased from said at least one media device

23 mission planning computer, and wherein the mission planning computer  
24 remains at a physical distance from the target computing device after  
25 commencement of the mission,

26 wherein after sensitive data is encrypted on at least one media  
27 device connected to the mission planning computer workstation, each of the  
28 at least one media devices are connected to the target portable computing  
29 device and the encryption key is resident only in volatile memory on any  
30 media device connected to the target portable computing device after  
31 mission commencement, and

32 wherein sufficient unencrypted data resides on at least one media  
33 device connected to the target portable computing device to enable the  
34 mission vehicle to return to a selected mission end location in the event that  
35 the encryption key is deleted from volatile memory on the target portable  
36 computing device during the mission.

1 13 (Currently Amended). A system as recited in claim 12, further  
2 comprising:

3 means for communication between the mission planning computer  
4 and at least one media device and target portable computing device,  
5 wherein the at least one media device is connected simultaneously to both  
6 the mission planning computer workstation and the target portable  
7 computing device prior to mission commencement and during data  
8 encryption.